



REN-ISAC

Research and Education Networking Information Sharing and Analysis Center

Membership
January 27, 2009

A Revised Membership Model

- In Feb 2009 a revised membership model will be implemented.
- Objectives of the new model are to:
 - Extend the reach of REN-ISAC more broadly in the R&E community
 - Retain a strongly trusted information sharing environment
 - Set a base for a long-term sustainable business model
 - Align “membership” directly with the institution

Membership Model

- Old model
 - Individuals joined to “represent [the] institution”. The individual is required to meet a certain work profile and receive trustworthiness vouches from existing members.
 - One tier or level of membership

Membership Model

- New model
 - Institutions and organizations join.
 - A CIO (or Head of IT) or designee joins on behalf of the institution. That person assumes the role of **management representative**, and nominates one or more **member representatives** who participate in the operational information sharing.
 - Two tiers of member representative participation are defined: **General** and **XSec**. The tiers differ in the criteria for membership, the degree of member representative vetting, and the classification of sensitive information shared in the tier.
 - An institution can have any combination of General and XSec representation.

Membership Model

- General member representatives:
 - The CIO (or Head of IT) nominates representatives – one or more full-time staff who meet eligibility requirements
- XSec member representatives:
 - To qualify for XSec, a General member representative must:
 - Have six weeks experience as a REN-ISAC General member representative
 - Be a principal security representative for the institution
 - Devote more than 50% of time to security work
 - Receive trustworthiness vouches from other XSec members
 - Submit an application
- All REN-ISAC members, as of Feb 1, 2009, have grandfathered XSec eligibility.

Membership Model

- (unchanged) Membership is open to:
 - institutions of higher education,
 - teaching hospitals,
 - research and education network providers, and
 - government-funded research organizations;
 - international, although focused on U.S.

General and XSec

Benefit	General	XSec
Receive and share practical defense information in a private trust community	sensitive	extra sensitive
Establish relationships with known and trusted peers	yes	yes
Have access to direct security services	some	yes
Benefit from information sharing relationships in the broad security community	yes	yes
Benefit from vendor relationships, such as the REN-ISAC and Microsoft Security Cooperation Program relationship	yes	yes
Participate in technical educational security webinars	yes	yes
Participate in REN-ISAC meetings, workshops, & training	yes	yes
Have access to the 24x7 REN-ISAC Watch Desk	yes	yes
Have access to threat information resources ("data feeds") that can be used for IP address and DNS block lists, signatures, identification of local compromised machines, etc.	limited	yes

Membership Fees

- The fee is per-institution, irrespective of the number of member representatives from the institution
- If one or more representatives at an institution are XSec, the institution pays the XSec fee
- Our business plan called for fees of \$900/700 XSec/General for the fiscal year beginning July 1, 2009, but due to the economic downturn, a decision has been made to scale back plans for fiscal 2009-10, and reduce fees by 50%.
- Accordingly, fees for fiscal 2009-10 are:
 - \$450/year for institutions with one or more XSec member representatives
 - \$350/year for General member-only institutions
- Billed in March
- Fees will be re-evaluated each year.

REN-ISAC Business Model

- Financial goal - Through a combination of tangible sponsorship, support, other philanthropic revenue, and fees, generate funding for sustainable REN-ISAC operations, supporting reach to all of U.S. higher education.
- All revenue generated by the REN-ISAC is used to fund services provided to the R&E community.
- Voluntary member contributions of staff time and expertise are used to keep fees as low possible.
- Financial principles and guidelines are published at <http://www.ren-isac.net/docs/charter.html>
- A financial review will be conducted once yearly with participation of the Executive Advisory Group.

Conversion to the New Model

- Mid-February
- Prepare: Identify management representative
 - CIO, head of IT, **or CISO** (CISO option for current members only)
- Prepare: Agreements
 - Mgmt rep: Terms & Conditions, and Information Sharing Policy
 - Member rep: Information Sharing Policy
- Entering Registry information – mgmt and member reps
- Plumbing
 - New mailing lists: General + XSec, and XSec only
 - New IRC: General + XSec, and XSec only
 - Changes to URLs of feeds: XSec only
 - No changes to wiki: General + XSec
- Budget for fee

References

- REN-ISAC Organizational Documents
 - Charter
 - <http://www.ren-isac.net/docs/charter.html>
 - Membership Document
 - <http://www.ren-isac.net/docs/membership.html>
 - Membership Terms and Conditions
 - http://www.ren-isac.net/docs/terms_and_conditions.html
 - Fees
 - <http://www.ren-isac.net/docs/fees.html>
 - Information Sharing Policy
 - http://www.ren-isac.net/docs/information_sharing_policy.html
 - Disclaimer
 - <http://www.ren-isac.net/docs/disclaimer.html>
- Overviews
 - Flier
 - http://www.ren-isac.net/docs/ren-isac_brief.pdf
 - Executive Overview
 - http://www.ren-isac.net/docs/ren-isac_executive_overview.pdf

Contacts

Executive Advisory Group, see <https://secure.ren-isac.net/eag/>

Jack Suess, Chair EAG, jack@umbc.edu

Mark Bruhn, Executive Director, mbruhn@iu.edu

Doug Pearson, Technical Director, dodpears@ren-isac.net

Gabriel Iovino, Principal Security Engineer, giovino@ren-isac.net

<http://www.ren-isac.net>

24x7 Watch Desk:

soc@ren-isac.net

+1 (317) 278-6630